SECRET
Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

8 DEC 1970

MEMORANDUM FOR: Chairman, Information Processing Board

SUBJECT : ADP Contingency Backup for CIA

A. Introduction

1. This memorandum deals with describing current procedures and recommending policy for providing backup support for CIA's computer centers in the event of a major equipment outage or the destruction of files/programs in one or more of those centers. The concern here is not how to re-establish a center such as restoring its electric power, but how to continue critical operations even though some damage has occurred to one or more components of the center. A major outage is defined as one that exists for more than several days and could last for up to 4 to 6 weeks. A major outage would most likely result from fire, severe water damage, or even possibly bomb damage. This paper is not concerned with providing backup in the event of a catastrophe such as nuclear attack, the assumption being that in that event ADP backup would not be a major concern.

2. The four major processing centers are of primary concern herein, i.e., OCS, CRS, RID, and NPIC. These centers have general purpose computing equipment and they perform a variety of different

SECRET
Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

kinds of applications for a broad spectrum of users. Aside from NPIC, these centers have compatible equipments. The single-or limited-purpose CIA computer operations, e.g., analog processing in OEL and message processing in OC, have unique equipments and software and are faced with somewhat different backup problems; but the general policies contained in this paper should also be applicable to those centers.

3. As indicated above, two aspects of backup support are examined herein: (1) hardware and (2) programs and files stored in machine language form. Hardware loss is not considered nearly as critical as software loss, i.e., computer manufacturers would provide all possible assistance to overcome hardware loss. Loss of software could lead to critical problems if a computer center does not have adequate backup recovery. If all files and programs including duplicates are stored in a single tape library and that tape library is destroyed, the only recourse is to re-establish files by rekeying out-of-date printouts and rewriting programs or hopefully locating some programs in punch card form in programmers' work areas. Some of the loss would never be recovered.

B. Current Procedures

The Agency has no current uniform policy regarding ADP backup. However, each of the computer centers has considered the problem and most have done some planning to assure limited operational

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

capability in event of an outage.

1. CRS

a. Hardware--CRS has a working arrangement with OCS wherein OCS will provide machine support as required to process and search CRS's bibliographic AEGIS file, the primary CRS machine file of user interest. AEGIS programs and files have been processed on OCS equipment, and CRS has used OCS backup on at least one occasion.

b. Programs and Files--A duplicate copy of all CRS programs is maintained in punch card form in a first floor storage area of the Headquarters building remote from the computer center. CRS also periodically duplicates its and CRS customer file tapes and stores them in a ground floor tape library remote from the main tape library. CRS has plans to store copies of its inherited files (i.e., bibliographic files which have no current inputs but which are still of value for retrieval purposes) at the Records Center. It is also looking into the feasibility of storing duplicate copies of its AEGIS data base at Records Center. In sum, CRS maintains all its programs and files

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

in the computer center and duplicates of all programs and files are stored in an area remote from the computer center. Selected files are also candidates for storage at Records Center.

2. RID

a. Hardware--No formal arrangements have been instituted for hardware backup support, but in event of an emergency, RID would expect assistance from OCS or CRS. RID is converting its IBM 1410 programs and files to IBM 360/50. Until this conversion is completed, RID feels that it would have considerable difficulty in finding backup support for its two 1410's.

b. Programs and Files--RID maintains duplicate copies of all its programs and files in a ground floor storage area remote from the computer center tape library. All of these files are updated on a periodic schedule. In addition, RID currently has complete manual backup for its name trace function and limited manual backup for its on-line Document Control System.

3. OCS

a. Hardware--OCS has several alternatives for hardware backup:

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

25X1A

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

Next 1 Page(s) In Document Exempt

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

4. NPIC

a. Hardware--When NPIC operated UNIVAC 490 equipment it had backup arrangements with NSA. Similar arrangements were not carried over when NPIC switched to the UNIVAC 494. The NPIC and NSA 494 configurations are so different it is questionable whether NPIC could utilize NSA for backup support. Aside from the fact that NPIC has dual 494's, no other backup arrangements exist.

b. Programs and Files--NPIC has no current plan to remotely store files or programs. There is some backup insurance in the physical arrangement of the NPIC system, i.e., the files are stored in drums on the first floor as well as in the tape library on the second floor and the programs are stored in drums on the second floor in a room separated from the tape library by a fire wall. Copies of many programs are also maintained by the programming staff on the fifth floor. (This latter situation is probably also true to some degree in the other centers.)

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

C. Recommended Backup Policy

1. Loss of ADP capability, particularly software, would be very serious--yet it is considered an unlikely possibility. The fact that it would be a serious loss accounts for the periodic attention given the subject of backup. The fact that it is a remote possibility accounts for the fact that most centers have not implemented more systematic backup programs. ADP backup can be very expensive in terms of equipment and personnel costs if it involves establishing remote computer centers for contingency purposes or duplicating all files following each file update. This paper agrees with earlier assessments that the unlikelihood of serious loss would not justify such measures.

2. The following recommended policies would appear to give us adequate backup insurance without additional significant cost.

a. Each of the computer centers should review its hardware backup plans. If existing arrangements are nonexistent or poorly defined, they should be established and formalized to the extent of determining how much support can be anticipated from another center. In addition, programs should be tested on the backup center's

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

hardware to ensure that they will run. In NPIC's case, it may be concluded after further study that no reasonable backup arrangements can be instituted.

b. Each computer center should maintain an alternate site for the storage of backup copies of programs and files. This alternate site should be remote from the tape library but within the same building, [redacted] in the case of NPIC and within the Headquarters building for the other centers. Within Headquarters building it should be determined whether a center can use another center's tape library for alternate storage, i.e., can OCS store tapes in CRS or RID. This procedure would not require the construction of alternate storage sites.

25X1A

c. Duplicate copies of all active computer programs should be maintained in an alternate storage site. Satisfactory alternate storage could consist of the storage of program punch card decks in programmer work areas.

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

d. It is the file builder's (customer's) responsibility to assess the value of a file, i.e., it is up to the DD/S to determine the effect of the loss of the payroll file and to inform the ADP Center as to a file's criticality. It is the computer center's responsibility to advise customers as to the problems of recovery from loss (e.g., availability of recent file printouts, etc.) and to advise whether backup file storage seems appropriate. All files do not require backup--some are transitory in nature, are not critical, or could be easily reconstructed. If a file is critical, two factors will generally dictate whether it should be backed up, i.e., (a) is the content recoverable from another source? and (b) if so, how long and how much effort would be required to reconstitute the file? It is recommended that OCS develop guidelines for file backup and using these guidelines, each of the computer centers undertake a file backup review in consultation with customers in order to implement a systematic file backup program for each center.

SECRET

Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

SECRET
Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7

e. Each center should annually review its contingency backup program and report the results of this review to the Chairman, Information Processing Boar[redacted]

ILLEGIB

25X1A

IP&E Team

SECRET
Approved For Release 2001/11/01 : CIA-RDP74-00390R000300320012-7